1

List Decoding of Reed-Solomon and Algebraic Geometry Codes

Tom Høholdt

Abstract— **We survey some of the recent work on list decoding of Reed- Solomon and algebraic geometry codes.**

Keywords— **List-decoding, Reed-Solomon Codes, Algebraic Geometry Codes**

I. Summary

In 1997 M. Sudan [1] presented a conceptually easy algorithm for decoding Reed-Solomon codes of rates less than $\frac{1}{3}$ beyond half the minimum distance. The method was extended to algebraic geometry codes by M.A.Shokrollahi and H.Wassermann in [2] and M.Sudan and V. Guruswami in [3] further improved the algorithm to cover all rates both for Reed-Solomon codes and for general algebraic geometry codes. It was clear from [3] that the resulting algorithms had polynomial complexity, but also that more work was needed to make the computations really efficient. This resulted in work by Refslund Nielsen and Høholdt [4], Feng and Blahut [5], Augot and Pecquet[6], Roth and Ruckstein[7] for Reed-Solomon codes and by Høholdt and Refslund Nielsen[8], Pequet[9], Gao and Shokrollahi[10]and Sakata[11] for algebraic geometry codes.

II. Sudan's algorithm

The most basic form of the algorithm for Reed-Solomon codes can be formulated as follows:
Let $L = \{f \in \mathbb{F}_q[x] \mid \deg(f) < k\}$
and $\mathbb{F}_q = \{\alpha_0, \alpha_1 \ldots, \alpha_{q-1}\}$.
The $(q, k, q-k+1)$ Reed-Solomon code C then is
$C = \{(f(\alpha_0), \ldots, f(\alpha_{q-1})) \mid f \in L\}$
The decoding algorithm , when a word $w \in \mathbb{F}_q^n$ is received has the following two steps;

- Calculate $Q_s(x,y) \in \mathbb{F}_q[x,y]\backslash\{0\}$ such that $Q(\alpha_i, w_i) = 0 \ i = 0, \ldots, q-1$ and $wdegQ \leq q - \tau - 1$ where $w(x) = 1$ and $w(y) = k-1$
- Factorize Q into irreducible factors.
- If $y - f(x)$ with $\deg(f) < k$ divides Q and $d(f(\alpha_0), \ldots, f(\alpha_{q-1}), w) \leq \tau$ then include $f(\alpha_0), \ldots, f(\alpha_{q-1})$ in the list.

Here $\tau = \lfloor \frac{(r-1)(2q-r(k-1))-1}{2r} \rfloor$
where r is the unique natural number satisfying
$\binom{r}{2} \leq \frac{q}{k-1} < \binom{r+1}{2}$

The output of the algorithm is a list of codewords of distance at most τ from the received word.
10cm

Department of Mathematics, Technical University of Denmark, Bldg 303 DK-2800 Lyngby Denmark, email tom@mat.dtu.dk

The results obtained in [4] - [11] give efficient implementations of this algorithm and its extensions.

On a more theoretical level the paper [12] by J.Justesen and T. Høholdt gives general bounds of the error-correcting capability of list decoders for MDS-codes.

References

[1] M.Sudan Decoding of Reed-Solomon codes beyond the error-correction bound. *J.Compl.*, 13 pp.180-193, 1997

[2] M.A.Shokrollahi, H.Wassermann List Decoding of Algebraic-Geometric Codes. *IEEE Trans. Inform. Theory* 45 pp432-437 march 1999

[3] V.Guruswami and M.Sudan Improved decoding of Reed-Solomon and algebraic-geometric codes In *Proceedings of the 39th IEEE Symposium on Foundations of Computer Science* 1998

[4] R.Refslund Nielsen , T. Høholdt Decoding Reed-Solomon Codes beyond half the minimum distance. *Proceedings of the International Conference on Coding Theory, Cryptography and Related Areas , Guanajuato , Mexico 1998* Springer Lecture Notes in Computer Science.

[5] W.Feng, R.E.Blahut Some results on the Sudan algorithm, *Procceedings of the 1998 IEEE International Symposium on Information Theory*

[6] D.Augot,L.Pecquet An alternative to Factorization:Speedup for SUDAN's Decoding Algorithm and its Generalization to Algebraic-Geometric Codes. *preprint INRIA* France 1999.

[7] R.M.Roth, G. Ruckenstein Efficient Decoding of Reed-Solomon Codes Beyond Half the Minimum Distance. Submitted to *IEEE Trans. Inform. Theory*nov. 1998

[8] T. Høholdt,R.Refslund Nielsen Decoding Hermitian Codes with Sudan's Algorithm. To appear in *Proceedings of AAECC-13* Springer Lecture Notes in Computer Science 1999

[9] L.Pecquet An algorithm to get some Factors of Bivariate Polynomials, without Factoring. *preprint INRIA* France 1999.

[10] S.Gao, M.A. Shokrollahi Computing Roots of Polynomials over Function Fields of Curves. *preprint ICSI Berkeley USA* june 1999

[11] S.Sakata A fast algorithm for constructing multivariate polynomials with preassigned zeroes. to appear in *Proceedings of the fifth conference on Finite Fields and applications* Augsburg 1999.

[12] J. Justesen , T. Høholdt Bounds on List Decoding of MDS Codes. Submitted to *IEEE Trans. Inform. Theory* april 1999.